REMARKS

Claims 1-20, 24-27, 35-42, 44 and 45 are pending in the present application. Claims 24 is amended above. Please cancel claim 44. No new matter is added by the claim amendments. Entry is respectfully requested.

Claims 1-9, 11, 14, 18, 19, 35, 37-40 and 42 stand rejected under 35 U.S.C. 102(e) as being anticipated by Downs, *et al.* (U.S. Patent Number 6,226,618). Claims 24, 25 and 27 stand rejected under 35 U.S.C. 102(e) as being anticipated by Mooney, *et al.* (U.S. Patent Number 6,351,813). Claims 26 and 45 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney, *et al.* in view of Bean, *et al.* (U.S. Patent Number 6,460,023). Claims 12, 13 and 15-17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, *et al.* in view of Horiike (U.S. Patent Number 6,744,905). Claim 20 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, *et al.* in view of Ciacelli, *et al.* (U.S. Patent Number 6,236,727). Claim 36 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, *et al.* in view of Mooney, *et al.* Claim 41 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, *et al.* in view of Paulson, *et al.* (U.S. Patent Number 5,585,585). Reconsideration of the rejection and allowance of claims 1-20, 24-27, 35-42 and 45 are respectfully requested.

In the present invention as claimed in independent claim 1, a method for preventing unauthorized use of digital content data to be transferred from a first system to a second system includes locating an archive of a digital content data at the first system, and determining transaction data of the second system that identifies the second system. The method further includes modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive and transferring the modified archive from the first system to the second system.

Downs, *et al.* discloses an electronic content delivery system in which a content provider(s) 101 uses a watermark to embed data in Content 113, such data including the content identifier, content owner and other information, such as publication date and geographic distribution region. This watermark is referred to in Downs, *et al.* as a "Copyright Watermark" 529. Upon reception, the End-User Device(s) 109 watermarks the copy of the Content 113, with the content purchaser's name and Transaction ID 535, and with other information such as date of license and Usage Conditions 517 (see Downs, *et al.*, FIG. 5, column 22, lines 10-24). This watermark is referred to in Downs, *et al.* as a "License Watermark" 527. Transaction Data 642 (see Downs, *et al.*, FIG. 6) provides user identity information to be included in the watermark of the Content 113 that is downloaded to the End-User(s) 109. The Transaction Data 642 includes the content purchaser's name, Transaction ID 535, date of license and Usage Conditions 517 (see Downs, *et al.*, column 76, lines 1-62). The Transaction ID 535 is downloaded to the End-User Device(s) 109 and used to watermark the Content 113 at the End-User Device(s) 109 (see Downs, *et al.*, column 22, lines 10-24).

Downs, *et al.* fails to teach or suggest "modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive" and "transferring the modified archive from the first system to the second system", as claimed in claim 1. Instead, in Downs, *et al.*, the Content 113 is embedded with Transaction Data of the End-User Device(s) 109 after reception of the Content 113 at the End-User Device(s) 109. Therefore, in Downs, *et al.*, a "modified archive" is not transferred "from the first system to the second system" as claimed in claim 1. Instead, in Downs, *et al.*, the Content 113 is modified at the recipient system (End User Device(s) 109) following transfer of the Content 113.

Accordingly reconsideration and removal of the rejection of claim 1 as being anticipated by Downs, *et al.*, are respectfully requested. With regard to dependent claims 2-9, 11, 14, 18, 19, 35, 37-40 and 42, it follows that these claims should inherit the

allowability of the independent claim from which they depend.

With regard to the rejection of claims 12, 13 and 15-17 as being unpatentable over Downs, *et al.* and Horiike, Horiike is cited in the Office Action as teaching creating a map of the increased memory allocation. Horiiki fails to teach or suggest "modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive" and "transferring the modified archive from the first system to the second system", as claimed in claim 1.

Downs, *et al.* and Horiike, whether alone or in combination, fail to teach or suggest "modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive" and "transferring the modified archive from the first system to the second system", as claimed in claim 1.

Accordingly, it is submitted that the combination of Downs, *et al.* and Horiike fails to teach or suggest the invention as claimed in claims 12, 13 and 15-17. Reconsideration of the rejection of, and allowance of, claims 12, 13 and 15-17 are respectfully requested.

With regard to the rejection of claim 20 as being unpatentable over Downs, *et al.* and Ciacelli, *et al.*, Ciacelli, *et al.* is cited in the Office Action as teaching that the second system replaces the false data by the original data segments immediately prior to execution of the corresponding memory locations, and replaces the original data by the false data immediately following execution of the corresponding memory locations. Ciacelli, *et al.* fails to teach or suggest "modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive" and "transferring the modified archive from the first system to the second system", as claimed in claim 1.

Downs, *et al.* and Ciacelli, *et al.*, whether alone or in combination, fail to teach or suggest "modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive" and "transferring the modified archive from the first system to the second system", as claimed in claim 1.

Accordingly, it is submitted that the combination of Downs, *et al.* and Ciacelli, *et al.* fails to teach or suggest the invention as claimed in claim 20. Reconsideration of the rejection of, and allowance of, claim 20 are respectfully requested.

With regard to the rejection of claim 36 as being unpatentable over Downs, *et al.* and Mooney, *et al.*, Mooney, *et al.* is cited in the Office Action as teaching a unique identifying value is used to create a system unique encryption key. Mooney, *et al.* fails to teach or suggest "modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive" and "transferring the modified archive from the first system to the second system", as claimed in claim 1.

Downs, *et al.* and Mooney, *et al.*, whether alone or in combination, fail to teach or suggest "modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive" and "transferring the modified archive from the first system to the second system", as claimed in claim 1.

Accordingly, it is submitted that the combination of Downs, *et al.* and Mooney, *et al.* fails to teach or suggest the invention as claimed in claim 36. Reconsideration of the rejection of, and allowance of, claim 36 are respectfully requested.

With regard to the rejection of claim 41 as being unpatentable over Downs, *et al.* and Paulson, *et al.*, Paulson, *et al.* is cited in the Office Action as teaching that if it is determined that the second system is an invalid recipient of the archive, further modifying the archive into the archive that causes an exit, and error condition, or communication to

another system entity which begins a cascading exit process, in the second system, and transferring the further modified archive to the second system. Paulson, *et al.* fails to teach or suggest "modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive" and "transferring the modified archive from the first system to the second system", as claimed in claim 1.

Downs, *et al.* and Paulson, *et al.*, whether alone or in combination, fail to teach or suggest "modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive" and "transferring the modified archive from the first system to the second system", as claimed in claim 1.

Accordingly, it is submitted that the combination of Downs, *et al.* and Paulson, *et al.* fails to teach or suggest the invention as claimed in claim 41. Reconsideration of the rejection of, and allowance of, claim 41 are respectfully requested.

With regard to the rejection of claims 24, 25 and 27 as being anticipated by Mooney, *et al.*, in the present invention as claimed in independent claim 24, a method for preventing unauthorized use of digital content data hosted on a system includes, determining whether an unauthorized use of digital content data is in progress, and in the case where an unauthorized use is determined, initiating a defense action by disabling only an input device in association with the unauthorized use. The input device is only disabled in an unauthorized interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window.

It is stated in the Office Action at page 10, paragraph 3 that Mooney, *et al.* does not disclose expressly that the input device is only disabled in an unauthorized interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window.

- 13 -

Therefore Mooney, *et al.* fails to teach or suggest determining whether an unauthorized use of digital content data is in progress, and "in the case where an unauthorized use is determined, initiating a defense action by disabling only an input device in association with the unauthorized use, wherein the input device is only disabled in an unauthorized interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window", as claimed in claim 24.

Accordingly reconsideration and removal of the rejection of claim 24 as being anticipated by Mooney, *et al.*, are respectfully requested. With regard to dependent claims 25 and 27, it follows that these claims should inherit the allowability of the independent claim from which they depend.

With regard to the rejection of claims 26, 44 and 45 as being unpatentable over Mooney, *et al.* and Bean, *et al.*, Bean, *et al.* discloses a software authorization method which permits a developer to provide licensed software content files to a customer. In Bean, *et al.*, authorized content files are downloaded to users of a customer's site. Only content files embedded in the authorized Web pages or domain names may be displayed or executed on the users' computer. If the content is not authorized, the user views a watermark that indicates that a rich media asset is not properly licensed and that obstructs the display of the rich media asset or display an error message. In FIG. 4 of Bean, *et al.*, each of windows 70, 74 and 76 are counted as a single authorized use of the content so that there are three authorized uses. In Bean, *et al.*, the output of the content is obstructed or an error message is displayed during an unauthorized use.

Bean, *et al.* fails to teach or suggest determining whether an unauthorized use of digital content data is in progress, and "in the case where an unauthorized use is determined, initiating a defense action by disabling only an input device in association with the unauthorized use, wherein the input device is only disabled in an unauthorized

interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window", as claimed in claim 24. Instead, in Bean, *et al.*, the output of the content is obstructed or an error message is displayed during an unauthorized use. Therefore, an output device is disabled in an unauthorized window during an unauthorized use in Bean, *et al.*, rather than an "input device" as claimed in claim 24.

Mooney, *et al.* and Bean, *et al.*, whether alone or in combination, fail to teach or suggest determining whether an unauthorized use of digital content data is in progress, and "in the case where an unauthorized use is determined, initiating a defense action by disabling only an input device in association with the unauthorized use, wherein the input device is only disabled in an unauthorized interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window", as claimed in claim 24.
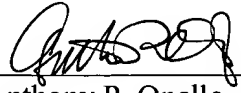
Accordingly, it is submitted that the combination of Mooney, *et al.* and Bean, *et al.* fails to teach or suggest the invention as claimed in claims 26 and 45. Reconsideration of the rejection of, and allowance of, claims 26 and 45 are respectfully requested.

Closing Remarks

It is submitted that all claims are in condition for allowance, and such allowance is respectfully requested. If prosecution of the application can be expedited by a telephone conference, the Examiner is invited to call the undersigned at the number given below.

Respectfully submitted,

Date: April 14, 2006

Mills & Onello, LLP
Eleven Beacon Street, Suite 605
Boston, MA 02108
Telephone: (617) 994-4900, Ext. 4902
Facsimile: (617) 742-7774
J:\ECD\0003\amendmentafterfinal.wpd

Anthony P. Onello, Jr.
Registration Number 38,572
Attorney for Applicant